Угрозы информационной безопасности: характеристика и способы противодействия.

Что такое информационная безопасность?

- Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации

Сколько людей на планете являются пользователями сети интернет?

- **8 105 616 187 человек - численность населения Земли**

- **5 310 221 130 человек являются пользователями**

Плюсы и минусы сети интернет

Плюсы:

+ Дистанционное обучение
+ Неограниченный доступ к информации
+ Работа
+ Бизнес и маркетинг
+ Общение и знакомства
+ Технологии

Минусы:

- Незаконная деятельность
- Вирусы
- Мошенничество в сети Интернет
- Повышение риска безопасности
- Интернет-зависимость
- Кибербуллинг
- Терроризм

Виды информационного воздействия

Информационно-техническое (объект воздействия информсистемы)

Информационно-психологическое (объект воздействия - люди)

Типы киберпреступлений

- Мошенничество с электронной почтой и интернет-мошенничество.
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации).
- Кража финансовых данных или информации с банковских карт
- Кража и продажа корпоративных данных
- Кибер-шантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Виды интернет мошенничества

- Взлом аккаунтов (мошенничество с электронной почтой и интернет-мошенничество)
- Фишинг - мошенничество с использованием личных данных (кража и злонамеренное использование личной информации)
- Травля в сети (кибербуллинг)
- Подозрительные знакомства (груминг)
- Сваттинг (введении аварийно-спасательной службы в заблуждение)
- Нежелательный контент
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)
- Азартные игры
- Трата родительских денег
- Вирусы

Фи́шинг

- Фи́шинг—вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.) логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.

Вишинг

- Вишинг—один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом / платежной картой.

Смишинг

- Сми́шинг—вид фишинга через SMS. Мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговые сайты мотивирующее её войти на этот сайт. Как вариант жертве предлагается отправить в ответном SMS сообщении конфиденциальную информацию, касающуюся платежных реквизитов или персональных параметров доступа на информационно-платежные ресурсы в сети Интернет.

СКАМ

- СКАМ -Вид интернет-мошенничества, когда злоумышленник сначала втирается к пользователю в доверие, а потом обманывает его. Чаще всего скамеры знакомятся с жертвой в социальных сетях, на форумах или сайтах знакомств.

Кибератака

- Кибератака —или хакерская атака —это вредоносное вмешательство в информационную систему компании, взлом сайтов и приложений, личных аккаунтов и устройств. Главные цели —получить выгоду от использования этих данных или шантажа владельцев. Есть целые хакерские группы, которые взламывают сайты, инфраструктуры и сервисы

Кибербуллинг

Кибербуллинг –это вид травли с применением интернет технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала. Это запугивание, унижение, травля, физический или психологический террор, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона и направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия. Все действия совершаются с использованием имейлов, сообщений в меседжерах и соцсетях, а также посредством выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.

Сваттинг

- Сватинг –тактика домогательства, которая реализуется посредством направления ложного вызова той или иной службе. Например, люди сообщают о минированиях, преследуя цель устроить неразбериху и панику в конкретном месте.

Цифровая гигиена

- Цифровая гигиена –этосвод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет.

Как не стать жертвой киберпреступления?

- Регулярно обновляйте ПО и операционную систему, также антивирусное ПО
- •Используйте сложные пароли •Не открывайте вложения в электронных спам-сообщениях •Не нажимайте на ссылки в электронных спам-сообщениях и на сайтах, которым не доверяете •Не предоставляйте личную информацию, не убедившись в безопасности канала передачи •Свяжитесь напрямую с компанией, если вы получили подозрительный запрос •Внимательно проверяйте адреса веб-сайтов, которые вы посещаете
- •Внимательно просматривайте свои банковские выписки

Базовые правила «общения» с телефонными мошенниками

- Основное правило: не сообщайте данные
- Перезвоните
- Задайте контрольный вопрос
- Никаких ссылок
- Не переводите деньги
- Не перезванивайте
- Ошибка перевода: свяжитесь с банком
- Проверяйте источники

Все эти правила базовые при общении с мошенниками, но каждый день изобретаются новые способы обмана.

- Если Вы все же стали жертвой киберпреступников, необходимо обращаться в «Управление К» МВД России, борющееся с преступлениями в сфере информационных технологий

Тел.: +7 (4742) 36–91–38

+7 (4742) 22–01–60

+7 (4742) 36–91–60

Спасибо за внимание!